BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-401

17 MAY 2011

Communications and Information

AIR FORCE ARCHITECTING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil/**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6PA

Certified by: SAF/A6P
(Mr. Bobby Smart, SES)

Supersedes: AFI33-401, 14 March, 2007

Pages: 20

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, *Enterprise Architecting*. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations. It supports the architecture-related mandates of the following Air Force Policy Directives (AFPD), Department of Defense Directives (DoDD), Chairman of the Joint Chiefs of Staff Instructions (CJCSI), and OMB Circulars: AFPD 33-1 *Information Resources Management*, 27 June 2006; AFPD 33-4, *Enterprise Architecting*, 27 June 2006; Office of Management and Budget (OMB) *Circular A-11, Preparation, Submission, and Execution of the Budget*; OMB Circular A-130, *Management of Federal Information Resources*; DoDD 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, May 05, 2004; DoDD 5000.01, *The Defense Acquisition System*, May 12, 2003; DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009; DoDI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, June 30, 2004; CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*, December 15, 2008; CJCSI 3170.01G, *Joint Capabilities Integration and Development System (JCIDS)*, March 1, 2009; AFI 63-101, *Acquisition and Sustainment Life Cycle Management*, April 17, 2009; and AFMAN 33-363, *Management of Records*, 1 March 2008.

This publication applies to all processes, services, systems, and procedures in support of decision making, transformation, and governance. It applies to all military and civilian Air Force personnel, members of the Air Force Reserve, Air National Guard, and individuals or activities as required by binding agreement with the Department of the Air Force. Field activities must

send proposed supplements to this instruction to Secretary of the AF, AF Chief Information Officer and Information Dominance (SAF/CIO A6) for review and approval prior to publication.

Send all recommendations for changes or comments to Secretary of the AF, AF CIO and Information Dominance (SAF/CIO A6), 1800 AF Pentagon, Washington DC 20330-1800, through appropriate channels, using AF IMT 847, *Recommendation for Change of Publication*. Ensure all records created as a result of processes prescribed in this publication are maintained IAW AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS).

See Attachment 1 for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed.

1. Air Force Architecting.

1.1. Relevance. The mandate to develop architectures comes from law (Clinger-Cohen Act, Title 10); Federal level requirements (OMB A-11, Federal Enterprise Architecture); DoD policies and instructions (DOD 5000.01, CJCSI 3170 and 6212); and the AF policies and instructions (AFPD 33-4, AFI 63-101). The intelligence community is also governed by Intelligence Community Directive (ICD) Number 1, "*Policy Directive for Intelligence Community Leadership*".

1.2. Purpose. Government agencies continually assess current performance, identify opportunities for performance improvement, and translate opportunities into specific actions. AF leaders are called upon daily to make decisions across the AF, often without being provided objective analysis of the second and third order impacts of their decisions. Enterprise architectures are formal blueprints for methodically and completely defining an organization's current (baseline) or desired (target) operational process and enabling environment. It is a tool that contains information for use by decision-makers in consideration of addressing and aligning enterprise-wide business plans and programs. Enterprise Architecture (EA) also helps all echelons to understand their alignment, key processes, roles, critical information, and supporting enablers. Thus, architecture is the key to understanding complexity and managing change; laying out the complexity of AF systems, processes and programs, and presenting decision-makers with clear articulated analysis.

Architecting provides a traceable connection from business strategy to each decision through implementation and deployment. This AFI provides the roles and responsibilities required to ensure all architectures are built for purpose, built to quality standards, enable analysis that can be used to support decision making, and guide transformation.

1.3. A Federated Approach. The AF uses a federated approach that partitions the AF Enterprise into an inter-related hierarchy of architectures (such as AF Service Core Function (SCF) architectures, Domain architectures, and Program architectures). AF Service Core Function architectures express the ways in which the Air Force is particularly and appropriately suited to contribute to national security. The SCF Architectures, along with the AF Business Support Services, depict the relationships between AF capabilities, functional support, and other DoD and external agencies. The Domain architectures are those architectures which reflect a segment of one or more AF Service Core Functions and depicting a set of capabilities and its associated missions, tasks, and their interrelationships. The Program architectures are those architectures which reflect the programs, systems and or services which provide IT support to the Domains and Service Core Functions. These architectures are developed and managed by various AF organizations (e.g., Service Core Function Lead Integrator Commands, Major Commands (MAJCOM), Field Operating Agencies (FOA), and Program Offices etc.). The specific focus and layered nature of the architectures facilitate allocation of responsibilities and enable architectures to be built autonomously. Architectures must be compliant with other interdependent architectures and the Air Force Enterprise Architecture (AFEA). Architectures in each successive layer must provide the detail necessary to fulfill its area of responsibility and articulate interdependencies to other architectures. An architecture that is certified as compliant with the AFEA can be used to certify compliance of subordinate architectures under certain conditions (see section 1.6.2. Architecture Certification), thus providing architecture certification reciprocity. In this way, an architecture at the lowest level of an enterprise is compliant with the highest federated level of an enterprise simply by complying with the level immediately above it. For the AF, this concept extends upward from the AFEA to Department of Defense (DoD) and Federal Enterprise Architecture (FEA) as the AFEA is deemed compliant with the DoD EA and the FEA.

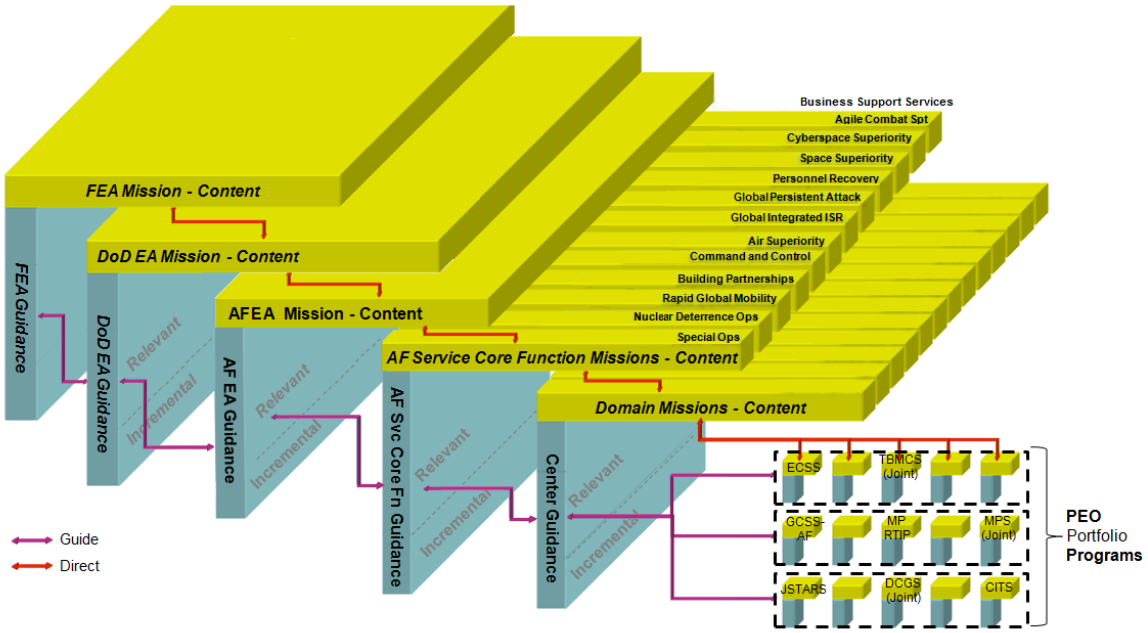
1.3.1. The architecture community leverages subject matter expertise throughout the AF, to enable the development of architectures that support analysis and decision making. We achieve this by using the appropriate perspectives to ensure a linkage between the service or component level strategy, associated objectives, performance measures, their related processes, and the activities (core, governing, and enabling) of the AF. This is accomplished by building architectures that follow the rules of AF architecting (e.g. architectures that fully address Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facility (DOTMLPF) considerations, address horizontal and vertical interdependencies, and are built to enable federation [federate-able]) as described in this instruction.

1.3.2. Designation of AF architecting areas of responsibility follows Figure 1 and begins with the AFEA which is assigned to the AF Chief Architect. Designation of architecting areas of responsibility at the next lower level is by AF Core Functions Lead Integrators (CFLIs) plus Business Support Services. The Business Support Services area is assigned to and managed by the AF Deputy Chief Management Office (DCMO). Lead Integrators

and DCMO will work with HAF/SAF Functionals to define architecture requirements for Service Core Functions and the Business Support Services area and the levels of decomposition of each. This will be reflected in their domain level architectures. At the domain level and below, architecting areas of responsibility lie with the MAJCOM and associated Program Offices. It is important to note that Domain architectures may support several SCFs, and likewise Program Architectures may support multiple Domains. It is the responsibility of the lead architecting organizations to ensure interfaces are negotiated appropriately to enable the Federated Approach.

1.3.3. Figure 1 - Architecture Federation depicts the AFEA relationship with architectures that are higher and lower in the hierarchy. The layers depicted run from the Federal Enterprise Architecture (FEA), through the DoD and the AF, down to an SCF level, a Domain Level which sub-divides any given SCF, and the Program Level where program architectures reside. Architectures in each layer must comply with the relevant rules for architecting, the relevant compliance criteria from above in the hierarchy that guide the content of the architecture (such as standards), and must represent operational interdependencies resulting in an architecture that is federate-able. An architecture is federated into architectures above in the hierarchy by the organization responsible for the architecture above in the hierarchy. This pattern must be followed down the hierarchy resulting in traceability from the Federal Enterprise Architecture to the program level architectures. The AFEA is built to be federate-able with DoD Enterprise Architecture and in turn the DoD EA is built to be federate-able to the FEA.

Figure 1. Architecture Federation.



1.3.4. The AF Enterprise Architecture. The AFEA, maintained by SAF/A6PA, does not exist in isolation, but is part of (and must conform to) the larger DoD EA and FEA. The AFEA defines how capabilities are met or intended to be met and documents processes and/or systems to support those capabilities. Enterprise architecting in the context of this

policy encompasses all activities involved in developing, certifying, approving, and using federated architectures at all levels of the Air Force. It includes information from other DoD, Intelligence and AF architectures, National Institute of Standards Module Validation List, National Information Assurance Partnership Validated Products List, DoD Metadata Repository, Net-Centric Enterprise Services Service Registry, DoD Issuances Website, DoD Enterprise Software Initiative Web Site, AF Enterprise IT Data Repository (EITDR), AF e-Publishing, DISR, the Infostructure Technology Reference Model (i-TRM), Federal Enterprise Architecture, DoD BEA, DoD IEA, DoD Strategic Management Plan, AF Strategic Plan, and the AF Strategic Management Plan. The AFEA registers its Overview and Summary Information (AV-1) with DARS, per OSD mandated requirement.

1.3.5. The Air Force Architecture Resource (AFAR). AFAR is the authoritative source for AF architecture information and is the repository for architecture data and metadata describing all approved, certified, and/or under-development AF architectures. Using AFAR in this way ensures full lifecycle traceability, as well as visibility of architectures from initial development through certification and approval. Additionally, the AFAR will include contact information on all architects throughout the AF.

1.3.6. The Defense Architecture Repository System (DARS). DARS-required metadata elements will be provided by each architecting organization submitting their architecture for approval and certification. SAF/A6PA will register the architecture and its associated required architecture metadata with DARS under the AF community after certification.

1.4. Using Architectures. The AF will use architecture to maximize its contribution to full spectrum dominance for the joint warfighter by supporting AF decision-making at all levels and guiding the transformations necessary to implement the decisions. AF architectures guide the transformations to ensure solutions support the business / mission need and deliver the required capability while supporting CIO requirements. For example, AF architectures will be used to ensure that proposed spending is optimized as appropriate and that solutions meet the targeted performance improvement upon which the decision to proceed was founded.

1.5. Building Architectures. The AF will build architectures specifically to support decision makers and decision making processes, and to guide potential transformation. The AF will build architectures to a minimum standard and must adhere to approved DoD architecture frameworks as directed by DoD or AF policy (e.g., DoDAF, etc.) or as appropriate (e.g., FEAF). Architectures will be developed to this minimum standard to ensure that a common set of information can be readily shared throughout the AF as described in this document. AF organizations must build architectures in accordance with a documented or referenced architecture development process and plan which must explicitly include meeting the needs of decision makers associated with the area of responsibility.

1.6. Governing Architectures. The AF will govern the quality of architecture and architecting activity through approval and certification processes to ensure that architectures are of significant quality for decision making and adhere to the rules of AF architecting.

1.6.1. Architecture Approval. AF Architectures will be approved as Fit for Purpose by designated Architecture Approval Authorities. Architecture Approval Authorities will be assigned by the owning MAJCOM or HAF/SAF Functional office with notification to the AF Chief Architect. The Architecture Approval Authority will direct a thorough review

of the architecture which includes stakeholders. The Architecture Review Process may be formal or informal depending on the scope of the project. The results of the review will be given to the Architecture Approval Authority, with a recommendation for approval or with recommended improvements.

1.6.1.1. Architecture approval criteria. Approval criteria are used to assess whether any given architecture is Fit for Purpose. Fit for Purpose also ensures an architecture has sufficient information to support decision making (such as DOTMLPF impacts, standards, and interoperability requirements; and that relevant laws, regulations and policies are adequately addressed). In addition, architectures must capture and represent the desired end state and performance with sufficient data to guide the transformation. Architecture Approval Authorities will provide a signed architecture approval letter indicating the architecture has been reviewed by an appropriate body of stakeholders and deemed Fit for Purpose. The architecture approval letter will have an attachment documenting the assessment leading to the architecture approval. The AF Architecture Approval letter template is available on the AFAR. The AF will not prescribe any given method for reviewing an architecture for approval as there are many methods available - each with their own strengths. For example, some openly available methods include: the Architecture Tradeoff and Analysis Method (ATAM), the Software Architecture Analysis Method (SAAM), and the Active Reviews for Intermediate Design (ARID) method. Specific architecture approval criteria are dependent on the given purpose of the architecture; however the list below is a good baseline:

1.6.1.1.1. Decision Making: Architecture should be assessed for completeness and accuracy in context to supporting specific decisions. Full DOTMLPF review is one dimension of completeness. Addressing the mission, information, service, and technology areas are another dimension. Additionally the architecture should be assessed for its accessibility to decision makers and/or their support staff. Additionally architectures should be used to identify gaps and redundancies across the enterprise to inform investment decisions.

1.6.1.1.2. Architecture Feasibility: The architecture should be assessed for technical feasibility, business feasibility, and financial feasibility.

1.6.1.1.3. Architecture Integrity: The architecture should be assessed for consistency between the mission/business, information, service, and technology areas and their connections.

1.6.1.1.4. Architecture Agility: The architecture should be assessed for its ability to accommodate alternatives based on changes in environment.

1.6.1.1.5. Interoperable: The architecture should be assessed to ensure that solution requirements for interoperability are appropriately represented and that standard interfaces (internal and external) utilize standardized vocabularies (reference DoDD 4630.8). Assertions for interoperability will be demonstrated and supported through the architecture as directed by the appropriate approval authority.

1.6.1.1.6. Dependable: The architecture should be assessed to ensure the solution

meets the requirement. This will be stated through performance measures based on OMB A-11 and Federal Enterprise Architecture (FEA) Consolidated Reference Model (CRM) requirements. These requirements and associated performance measures should address solution manageability, recoverability and serviceability.

1.6.1.1.7. Useable: The architecture should be assessed for human factors (Section 508, ADA), including hardware, software, and human systems (computer and machine) integration and interactions.

1.6.1.1.8. Prepared for Certification: The architecture should be assessed against certification criteria. The certification assertions should be prepared using the certification scorecard (available on AFAR) as an input to the certification process.

1.6.1.1.9. Security: The architecture should be assessed for adequate representation of security issues to support trusted relationships with partners driven by policy.

1.6.1.1.10. Technically Compliant: The architecture should be assessed from a technical and overall design perspective seeking to understand whether the right technical approaches are being applied for the given solution requirements and whether the collection of technologies will work together seamlessly.

1.6.1.1.11. Compliant with appropriate Law, Regulation and Policy (LRP): Architecture will address the LRPs and their associated review, inspection, or audit requirements based on the architectures stated purpose and scope.

1.6.1.1.12. Stakeholder Involvement: The stakeholders are included in the approval process, for example, AFSPC/AFNIC for capacity, compliance, and supportability.

1.6.2. Architecture Certification. AF Architectures will be certified by the Air Force Chief Architect or a designated Architecture Certification Authority. Certification is required for any architecture that has interdependencies with other architectures. Certification ensures architectures address AF rules for architecting, as presented in the AF Enterprise Architecture (AFEA) Compliance Guidance to meet interoperability support requirements as the AF moves toward an optimal set of capabilities.

1.6.2.1. The goal of AF Architecture Certification is to maintain a minimum common standard of Architecture across the Air Force. Accomplishing this goal will assist the AF Architecture to achieve multiple objectives:

1.6.2.1.1. The architecture meets a minimum common standard.

1.6.2.1.1.1. Discoverable information assets are captured in the Architecture.

1.6.2.1.1.2. Reusable information assets are captured in the Architecture.

1.6.2.1.2. The architecture has addressed appropriate compliance requirements.

1.6.2.1.3. The architecture is Fit-for-Federation (F4F).

1.6.2.1.3.1. The architecture supports decisions at or above the program level.

1.6.2.1.3.2. The architecture support analysis (i.e. such as interoperability, redundancy, DOTMLPF impacts, etc.).

1.6.2.1.3.3. The Federation of architectures provides a means to address Air Force Organization / Enterprise issues.

1.6.2.2. Certification of architectures is intended to streamline the architecture development process over time by reducing rework and lowering costs of integration and interoperation.

1.6.2.3. The Architecture Certification Authority will provide a signed architecture certification letter indicating the architecture has been reviewed and that the architecture meets / does not meet minimum criteria for certification. The architecture certification letter will have an attachment documenting the certification results which will be presented in a scorecard that rates the architecture against each criterion. This scorecard will note any material weaknesses found in the assessed architecture, along with a "get well plan" that describes the criteria / requirements that need to be addressed. The scorecard and any associated "get well plan" will comprise the attachment. The Certification Letter and Scorecard templates are available on the AFAR.

1.6.2.4. Certification will address the following eight (8) criteria:

1.6.2.4.1. Architecture Approval process was conducted: The architecture has been approved based on specific criteria and approval has followed a documented process.

1.6.2.4.2. The Architecture content is valid: The architecture contains valid data/information.

1.6.2.4.3. Architecture is positioned to support decisions: The architecture has been assessed for how it supports the defined consumers (purpose) and decisions it will be informing.

1.6.2.4.4. Architecture is positioned to be federated within the Air Force Enterprise Architecture: Architecture has related or aligned subordinate and parent architectures via the mapping of common architecture information. Architecture artifacts are visible and accessible to analysts, planners and decision makers at all levels.

1.6.2.4.5. Architecture is compliant with laws, regulations, and policies: The architecture has addressed compliance requirements based on the stated purpose and scope.

1.6.2.4.6. Architecture meets a minimum standard (discovery and use): The architecture has been developed to a minimum standard of architecting to ensure architecture information is authoritative, discoverable and useable.

1.6.2.4.7. Architecture meets a minimum AF standard (traceability): The architecture has been developed to a minimum standard to deliver auditable processes that maintain traceability from NEED to Deployed Capability - the solution meets the architecture and the need!

1.6.2.4.8. Architecture is under configuration control: The architecture is static upon approval and has identified a process to evolve and maintain configuration of architecture information.

1.6.2.5. AF architecture certification results will be reported through AFAR. This will include the certification letter and associated certification scorecard with results.

1.6.2.6. Designating Additional Certification Authorities. The AF Chief Architect is the primary architecture certification authority and will certify AF architectures. To enable tiered-accountability, the AF Chief Architect may delegate authority to architecting organizations at lower levels of the AF Enterprise to certify subordinate architectures. Organizations will not certify architectures they have created or sponsored themselves as those must be submitted to the next higher certification authority.

1.7. IT and NSS Standards. As with DoD architectures and the AFEA, adherence to approved technical standards is required. The DoD IT Standards Registry (DISR) mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. In accordance with DoDI 4630.8 *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, and AFI 63-101 *Acquisition and Sustainment Lifecycle Management*, all AF architectures shall use the DoD-mandated IT standards found in the DISR.

1.7.1. To add, update or delete a standard currently in the DISR, a change request must be submitted to the DISR for consideration by DISR Technical Working Group representatives after coordination with SAF/A6PA. To use an emerging or retired standard or to disregard a DoD-mandated IT standard requires a waiver. The process for change requests or waivers is available on the AF Information Technology Standards Management web site (see references).

1.7.2. Infostructure Technology Reference Model (i-TRM): In addition to the DISR, the i-TRM is the AF's authoritative source for enterprise standard IT products, computer configurations, platform and service profiles, technical solutions and standard configurations of software and hardware. AF will use products from the standard product list or receive a waiver from A6/CIO.

2. Roles and Responsibilities.

2.1. This AFI establishes eight general roles (2.1.1 - 2.1.8) and four specific roles (2.2 - 2.5) for architecting. These general roles are independent of the scope of a given architecture (Headquarters United States AF (HAF) Functionals, MAJCOMs, Program Management Offices, etc).

2.1.1. An Architect analyzes, defines, builds, maintains, and/or improves an architecture for a stated purpose. Architects:

2.1.1.1. Support decision makers in area of responsibility with architecture data and analysis.

2.1.1.2. Assist users and other architects with understanding the subject architecture to ensure an accurate reflection of interdependent capabilities and requirements for related architectures.

2.1.1.3. Develop and maintain architecture for area of responsibility in accordance with this publication

2.1.1.4. Follow a documented change management process as defined by architecting management.

2.1.1.5. Evaluate commercial products related to architecture and document evaluation of suitability.

2.1.1.6. Develop technical forecasts related to architecture.

2.1.1.7. Stay current in tools, methods, and frameworks; and maintains all required certifications.

2.1.1.8. Identify, document, assess, and develop a standard profile related to their architecture.

2.1.1.9. Obtain approval recommendation from the Architecture Review Board (ARB)

2.1.1.10. Submit approved architecture to the Architecture Certification Authority for certification.

2.1.2. A User of architecture employs architecture and/or architecture analysis to support decision making. In addition, the user exploits architecture to simplify complexity, reveal interdependent relationships, identify DOTMLPF gaps, eliminate redundancy and maximize resource allocation.

2.1.3. An Architecture Review Board assesses architectures against Fit for Purpose criteria.

2.1.3.1. The review board may be formal (chartered) or informal, based on the needs of the organization and the purpose and scope of the architecture. For example, organizations may opt to use existing coordination processes and tools in lieu of standing up a formal board, with the approval of the Architecture Approval Authority.

2.1.3.2. Every organization that sponsors an architecture will conduct a review of the architecture, whether at the AFEA, SCF, or lower level.

2.1.3.3. This review will include the owner of the architecture and stakeholders.

2.1.3.4. The results of the review will be a recommendation for approval from designated Architecture Approval Authority, or recommended changes to the architecture to obtain approval.

2.1.4. An Architecture Approval Authority accepts and signs an architecture as Fit for Purpose.

2.1.4.1. The Architecture Approval Authority directs a thorough review of the architecture to determine if it is Fit for Purpose.

2.1.4.2. If warranted, the Architecture Approval Authority accepts and signs the architecture approval letter and requests certification.

2.1.4.3. The Approval Authority will document and publish the assessment results and approval letter on AFAR.

2.1.5. An Architecture Certification Reviewer plans, organizes, and conducts an assessment of architectures against AF architecting criteria. Reviewers recommend action as to certification to **the Architecture Certification Authority.** Results will be documented and published on AFAR.

2.1.6. The Architecture Certification Authority accepts and signs an architecture as compliant with **AF achitecture certifying criteria.**

2.1.6.1. Sends a letter with results to the owner of the architecture and the Architecture Approval Authority.

2.1.6.2. Delegates authority to certify subordinate AF architectures to other subordinate AF organizations with the approval of AF Chief Architect.

2.1.7. Architecting Management plans, organizes, and resources architecting activities. They:

2.1.7.1. Place the architecture under configuration control.

2.1.7.2. Publish, approved and under-development architecture metadata to AFAR.

2.1.7.3. Oversee architecture review process and submit recommendation to the Architecture Approval Authority.

2.1.7.4. Ensure architects are trained, and define training and certification requirements for local teams.

2.1.8. Architect Trainer provides education on architecting within the AF.

2.2. HAF/SAF Functionals, SCF Lead Integrators, MAJCOMs must ensure their areas of responsibility are architected. In addition to all other applicable roles, these organizations must:

2.2.1. Participate with SAF/A6PA on establishing and maintaining architecture use policy - representing needs of decision makers.

2.2.2. Plan for and provide financial, manpower, and other resources as needed to carry out their architecting responsibilities.

2.2.3. Appoint a lead to oversee architecture development activities in area of responsibility, ensure architecture compliance, and participate in architecture governance bodies.

2.2.4. Develop and use approved architecture data and/or analysis to support decision making.

2.2.5. Ensure Classification and Distribution Statement meet operational/mission and classification requirements.

2.2.6. Provide AF representation, as required, on DISR technical working groups for review and disposition of technical standards in support of SAF/A6 and Air Force Space Command in their network management role.

2.2.7. Ensure efforts lead by Communities of interest and subordinate organizations are appropriately architected.

2.2.8. Participate in other Architecture Review processes in which they are a stakeholder (e.g. information exchange, network supportability, compliance issues).

2.2.9. Will include HQ AFSPC, as lead command for Cyber, in all Architecture Review processes as the stakeholder for capacity and supportability on AF networks.

2.3. The AF CIO will:

2.3.1. Appoint the AF Chief Architect.

2.3.2. Establish the AF Chief Architect as the AF Architecture Certification Authority.

2.3.3. Establish under the Chief Architect, an office responsible for the AFEA and AF architecting policy.

2.4. The AF Chief Architect will:

2.4.1. Oversee the AFEA development.

2.4.2. Ensure the AFEA complies with DoD architecture.

2.4.3. Participate in architecture governance bodies.

2.4.4. Submit the AFEA to the CIO for approval and release.

2.4.5. Certify AF architectures or delegate authority to certify AF architectures to other AF organizations.

2.5. The Office of the Chief Architect of the AF will:

2.5.1. Build and maintain the AFEA.

2.5.2. Operate, maintain and provide the AFAR.

2.5.3. Serve as the AF liaison to DARS and post appropriate sections of architectures in DARS.

2.5.4. Serve as the AF Representative to the DoD IT Standards Committee (ITSC).

2.5.5. Serve as the AF approval authority for waivers to the DISR.

2.5.6. Represent the AF on activities associated with the Military Communications-Electronics Board.

2.5.7. Review and certify all JCIDS and ISP architectures prior to AFROC review.

2.5.8. Sponsor and establish architecture education and training requirements and oversee and support the development and maintenance of those requirements.

2.5.9. Represent AF on DoD and academic teams establishing architecture certification requirements.

2.5.10. Assess and recommend certification of architectures (whole or part) to the AF Chief Architect; establish candidate criteria for compliance with law, DoD Directives, Joint Staff Instructions, and AF Policy.

2.5.11. Establish governance to oversee the adjudication, development, assessment, alignment, approval, compliance, maintenance, and application of the AFEA and subordinate architectures.

2.5.12. Establish or amend policy and/or guidance, as necessary, on the use of architectures (to include architecture information requirements and acceptance criteria) to support the AF decision making processes.

2.5.13. Publish and Maintain AFMAN(s) on AF Architecting.

2.5.14. Organize and coordinate architecture federation activities both internal and external to the AF enterprise.

2.5.15. Review and certify all JCIDS and ISP architectures prior to AFROC review.

3. Information Collections, Records, and Forms.

3.1. Information Collections. No information collections are created by this publication.

3.2. Records. Records pertaining to architectures created by this publication are retained and disposed of according to AFMAN 33-363, *Management of Records*, and disposed of in accordance with the AF Records Disposition Schedule (RDS).

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and Chief
Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

A Practical Guide to Federal Enterprise Architecture, Version 1.0, February 2001 (**http://www.gao.gov/bestpractices/bpeaguide.pdf**)

AF Enterprise Architecture (AFEA) Compliance Guidance Guide

AFI 63-101, Acquisition and Sustainment Life Cycle Management, April 17, 2009

AFMAN 33-363, *Management of Records* 1 March 2008

AFPD 33-4, Enterprise Architecting, 27 June 2006

AFPD 33-1 Information Resources Management, 27 June 2006

AFRIMS RDS at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**

Architecture Tradeoff and Analysis Method (ATAM), **http://www.sei.cmu.edu/architecture/tools/atam**/

Active Reviews for Intermediate Design (ARID) method, **http://www.sei.cmu.edu/architecture/tools/arid**/

CJCSI 3170.01G, Joint Capabilities Integration and Development System (JCIDS), 1 March 2009

CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December, 2008

DoD Architecture Framework (DoDAF), Version 2.0, DoD Federated Joint Architecture Working Group: **http://cio-nii.defense.gov/sites/dodaf20**/

DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004

DoDD 5000.01, The Defense Acquisition System, May 12, 2003

DoDD 8000.01, Management of the Department of Defense Information Enterprise, February 10, 2009

DoDI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), June 30, 2004

Federal Enterprise Architecture Consolidated Reference Model (FEA CRM) **http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf**

FEA Practice Guidance (Federal Enterprise Architecture PMO, OMB, dated Nov 2007) **http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_Practice_Guidance_Nov_2007.pdf**

OMB Circular A-11, Preparation, Submission, and Execution of the Budget, June 26, 2008

OMB Circular A-130, Management of Federal Information Resources, November 28, 2000

Software Architecture Analysis Method (SAAM), **http://www.sei.cmu.edu/library/abstracts/whitepapers/icse16.cfm**

Prescribed Forms

No forms are prescribed by this publication.

Adopted Forms

AF Form 847, Recommendation for Change of Publication.

Abbreviations and Acronyms

ACAT—Acquisition Category

AETC—Air Education and Training Command

AF—Air Force

AFAR—Air Force Architecture Resource

AFDD—Air Force Doctrine Document

AFEA—Air Force Enterprise Architecture

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Material Command

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

ARB—Architecture Review Board

BEA—Business Enterprise Architecture

C2—Command and Control

CCA—Clinger Cohen Act of 1996

CFLI—Core Function Lead Integrator

CIO—Chief Information Officer

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CONOPS—Concept of Operations

CoP—Community of Practice

DCMO—AF Deputy Chief Management Office

DISR—DoD IT Standards Registry

DoD—Department of Defense

DoDAF—DoD Architecture Framework

DoDD—DoD Directive

DoDI—DoD Instruction

DOTMLPF—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities

EA—Enterprise Architecture

EITDR—AF Enterprise IT Data Repository

ESI—Enterprise Software Initiative (DoD)

FEA—Federal Enterprise Architecture

FJAWG—Federated Joint Architecture Working Group

GIG—Global Information Grid

GOSG—General Officer Steering Group

HAF—Headquarters United States Air Force

IA—Information Assurance

IAW—In Accordance With

IEA—Information Enterprise Architecture

IMT—Information Management Tool

IS—Information System

IT—Information Technology

i-TRM—AF Infrastructure Technology Reference Model

ITSC—IT Standards Committee

JCIDS—Joint Capabilities Integration and Development System

JP—Joint Publication

MAJCOM—Major Command

MDR—DoD Metadata Repository

NCES—Net-Centric Enterprise Services

NIAP—National Information Assurance Partnership

NIST—National Institute of Standards

NSS—National Security System

OMB—Office of Management and Budget

OSD—Office Secretary of Defense

RDS—Records Disposition Schedule

SAF—Secretary of the Air Force

SCF—Service Core Function

USC—United States Code

Terms

Air Force Architecting—Applying architectural principles and processes across the Air Force Enterprise. (new).

Air Force Architecture Compliance Criteria—Minimum requirements that must be met by an AF architecture. These requirements are part of the AFEA and available in the AFEA on AFAR. (new).

Air Force Architecture Resource (AFAR)—The authoritative source of architecture data, policy, guidance, and reference material for the United States Air Force. (**https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-EA**).

Air Force Enterprise Architecture (AFEA)—An architecture that describes the Air Force Enterprise. The AFEA includes internal Air Force elements and processes and their relationships. The AFEA also defines external relationships between the Air Force Enterprise and external enterprises (such as DoD, US Navy, etc.). (AFPD 33-4).

Air Force Records Disposition Schedule (RDS)—is outlined in AFMAN 33-363, *Management of Records*, and is located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

AF Information Technology Standards Management—**https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-RQ-CA-01**

Architecture—(1) The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. (ISO/IEC 42010:2007/IEEE STD 1471-2000). (2) The structure of components, their relationships and the principles and guidelines governing their design and evolution over time. (DoDD 4360.05), (CIO Council, *A Practical Guide to Federal Enterprise Architecture*).

Architecture Framework—A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (Adapted from Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*).

Capability—The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) to perform a set of tasks to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a joint DOTMLPF change recommendation. In the case of materiel proposals/documents, the definition will progressively evolve to DOTMLPF performance attributes identified in the capability development document and the capability production document. (CJCSI 3170.01G).

Core Function Lead Integrator (CFLI)—A CSAF-designated organization which acts as the principal integrator for its assigned SCF and the corresponding CFMP. (NEW: Provided by SAF/A8)

DoD IT Standards Registry (DISR)—DoD Information Technology Standards Registry (DISR). The DISR (**https://disronline.disa.mil**) provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DoD systems. Use of the DISR is mandated for the development and acquisition of new or modified

fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture. (DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), April 23, 2007).

DoD Architecture Framework (DoDAF)—The overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate DoD managers at all levels to make key decisions more effectively through organized information sharing across Department, Joint Capability Areas (JCAs), Component, and Program boundaries. DoDAF V2.0 focuses on architectural data as information required by key DoD decision makers, rather than on developing individual products. The framework also enables architecture content to be built that is "Fit-for-Purpose", as defined and described in Section 1.4. DoDAF is one of the principal pillars supporting the responsibilities Department of Defense Chief Information Officer (DoD CIO) in exercise of his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. (DoD Architecture Framework Version 2.0, Volume 1: Introduction, Overview, and Concepts, Managers Guide, 28 May 2009)

Enterprise—An organization supporting a defined business scope and mission. An enterprise includes interdependent resources (people, organizations, and technology) that must coordinate their functions and share information in support of a common mission (or set of related missions). (Federal CIO Council, *A Practical Guide to Federal Enterprise Architecture*).

Enterprise Architecture (EA)—The explicit description and documentation of the current and desired relationships among business and management processes and supporting resources (e.g., IT, personnel). It describes the "current architecture" and "target architecture," to include the rules, standards, and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. (AFPD 33-1, *Information Resources Management*).

Federated Architecture—A loosely coupled collection of information assets that accommodates the uniqueness and specific purpose of disparate architectures and allows for their autonomy and local governance while enabling the enterprise to benefit from their content. It provides an approach for aligning, locating, and linking disparate architectures and architecture information via information exchange standards to deliver a seamless outward appearance to users. Its content describes mission capabilities and the IT capabilities necessary to respond to changing mission needs. (Adapted from DoD Federated Joint Architecture Working Group (FJAWG)). Adjective form: Federate-able – Fit for Federation.

Fit-For-Purpose—an assessment to ensure the quality of data in the architecture supports the appropriate decision-making process and guides the transformation effort. This should be

accomplished through stakeholder review of the architecture data. (Air Force Architecting Concept of Operations)

Information Technology (IT)—Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by a DoD Component directly, or used by a contractor under a contract with the DoD Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS). (DoD 4360.05).

Joint Capabilities Integration and Development System (JCIDS)—A Chairman of the Joint Chiefs of Staff process to identify, assess, and prioritize joint military capability needs. The JCIDS process is a collaborative effort that uses joint concepts and integrated architectures to identify prioritized capability gaps and integrated DOTMLPF solutions (materiel and non-materiel) to resolve those gaps. (CJCSI 6212.01E).

National Security System (NSS)—Any telecommunications or information system (IS) operated by the U.S. Government, the function, operation, or use of which: 1) involves intelligence activities; 2) involves cryptologic activities related to national security; 3) involves command and control of military forces; 4) involves equipment that is an integral part of a weapon or weapon system; or 5) is critical to the direct fulfillment of military or intelligence missions: (this does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics and personnel management applications). (DoDD 8000.01, 40 USC 11103) NOTE: For IA purposes only, pursuant to AFPD 33-2, *Information Assurance (IA) Program*, the term NSS also includes any telecommunications or IS that is protected at all times by procedures established for managing classified information. (44 USC 3542(2), DoDD 4360.05).

Process—A functionally or temporally linked collection of structured activities/ tasks aimed at producing specific services and products for an end-user. (DoDAF v2.0, Vol II, Table 2.4.1-2: Aliases and Composite Terms Related to Activities)

Program—A directed, funded effort, designed to provide a new, improved, or continuing, materiel, weapon, or information system capability in response to a validated operational or business need that supports operational requirements. (NOTE: For the purposes of this publication, this term is used interchangeably with the definition for Acquisition Program as defined in DoDD 5000.01), (AFPD 33-4).

Service—A mechanism to enable access to a set of one or more capabilities , where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description. (DoDAF 2.0).

Service Core Functions (SCF)—Functional areas that delineate the appropriate and assigned core duties, missions, and tasks of the Air Force as an organization, responsibility for each of which is assigned to CFLIs. SCFs express the ways in which the Air Force is particularly and

appropriately suited to contribute to national security, but they do not necessarily express every aspect of what the Air Force contributes to the nation. (NEW: Provided by SAF/A8).

Standards Profile—An architecture Standards Profile is the set of rules that governs system implementation and operation. In most cases, especially in describing architecture with less than a department-wide scope, building a Standards Profile will consist of identifying the applicable portions of existing standards guidance documentation, tailoring those portions in accordance within the latitude allowed, and filling in any gaps. This architecture view references the technical standards that apply to the architecture and how they need to be, or have been, implemented. The profile is time-phased to facilitate a structured, disciplined process of system development and evolution. Time phasing also promotes the consideration of emerging technologies and the likelihood of current technologies and standards becoming obsolete. (A Practical Guide to Federal Enterprise Architecture, V1.0).

Tiered-accountability - Tiered Accountability (TA)—is the distribution of authority and responsibility to a DoD organization for an element of the DoD EA. Under TA, DoD is defining and building enterprise-wide capabilities that include data standards, business rules, enabling systems, and an associated layer of interfaces for Department, specified segments of the enterprise (e.g., JCA, DoD Components), and Programmatic solutions. Each tier has specific goals, as well as responsibilities to the tiers above or below them.